UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/312,150	05/14/1999	PHILIP J. MIRE	M-7219-US	2203

7590 03/24/2004

DAVID L. McCOMBS
HAYNES and BOONE, LLP
901 MAIN STREET
SUITE 3100
DALLAS,, TX 75202-3789

EXAMINER	
MOORTHY, ARAVIND K	

ART UNIT	PAPER NUMBER
2131	15

DATE MAILED: 03/24/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/312,150	MIRE, PHILIP J.	
	Examiner	Art Unit	
	Aravind K Moorthy	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *30 January 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-29* is/are pending in the application.

4a) Of the above claim(s) *2,3,6,13,14,17,24,25 and 28* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,4,5,7-12,15,16,18-23,26,27 and 29* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *30 January 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-29 are pending in the application.

2. Claims 2, 3, 6, 13, 14, 17, 24, 25 and 28 have been cancelled.

3. Claims 1, 4, 5, 7-12, 15, 16, 18-23, 26, 27 and 29 have been rejected.

Continued Examination Under 37 CFR 1.114

4. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 3/26/03 has been entered.

Response to Arguments

5. Applicant's arguments with respect to claims 1-25 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

6. Claims 1, 4, 5, 7, 8, 12, 15, 16, 18, 19, 23, 26, and 27 are rejected under 35 U.S.C. 102(b) as being anticipated by Lipner et al U.S. Patent No. 5,557,346.

As to claims 1, 12 and 23, Lipner et al discloses generating a session. Lipner et al discloses encrypting the data utilizing the session key [column 11, lines 13-20]. Lipner et al

discloses encrypting the session key utilizing a user public key [column 11, lines 21-23]. Lipner et al discloses encrypting the session key utilizing a master public key [column 11, lines 27-29]. Lipner et al discloses generating a data packet including the encrypted data. Lipner et al discloses that the encrypted session key utilizes the user public key and the encrypted session key utilizing the master public key. Lipner et al discloses transmitting the data packet to a destination data processing system [column 11, lines 34-48]. Lipner et al discloses decrypting the data packet utilizing the session key [column 11, lines 54-60]. Lipner et al discloses decrypting the session key utilizing a user private key. Lipner et al discloses encrypting the encrypted session key utilizing a master private key [column 12, lines 29-58].

As to claims 4, 15 and 26, Lipner et al discloses encrypting the session key utilizing an asymmetric encryption routine [column 9, lines 47-57].

As to claims 5, 16 and 27, Lipner et al discloses encrypting the data utilizing a symmetric encryption routine [column 11, lines 34-42].

As to claims 7 and 18, Lipner et al discloses storing a user's private key on a data storage medium coupled to the destination data processing system [column 12, lines 29-39].

As to claims 8 and 19, Lipner et al discloses storing the master private key on a data storage medium coupled to the destination data processing system [column 12, lines 40-58].

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims 9, 10, 20 and 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lipner et al U.S. Patent No. 5,557,346 as applied to claims 1 and 12 above, and further in view of Dillaway et al U.S. Patent No. 5,742,756.

As to claims 9 and 20, Lipner et al does not teach retrieving the user's private key from a smart card utilizing a smart card reader coupled to the destination data processing system.

Dillaway teaches private key stored on a smart card utilizing a smart card reader coupled to the destination data processing system [figure 2].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Lipner et al so that the user's private key is stored on a smart card coupled to the destination node. The private key is only retrieved when the smart card is inserted into the smart card reader.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Lipner et al by the teaching of Dillaway because it utilizes a smart card to perform critical cryptography operations. The smart Card can be programmed or otherwise configured to never expose the user's private keys. Rather than providing a private key to the user's computer, the key is held within the smart Card, and required cryptographic operations are performed on the smart Card itself. This makes it impossible for hostile code to obtain the private key [column 3, lines 24-31].

As to claims 10 and 21, Lipner et al does not teach retrieving the master private key from a smart card utilizing a smart card reader coupled to the destination data processing system.

Dillaway teaches private key stored on a smart card utilizing a smart card reader coupled to the destination data processing system [figure 2].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified the Burke-Schneier combination so that the master private key is stored on a smart card coupled to the destination node. The master private key is only retrieved when the smart card is inserted into the smart card reader.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Lipner et al by the teaching of Dillaway because it utilizes a smart card to perform critical cryptography operations. The smart card can be programmed or otherwise configured to never expose the user's private keys. Rather than providing a private key to the user's computer, the key is held within the smart card, and required cryptographic operations are performed on the smart card itself. This makes it impossible for hostile code to obtain the private key [column 3, lines 24-31].

8. Claims 11, 22 and 29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lipner et al U.S. Patent No. 5,557,346 as applied to claims 1, 12 and 23 above, and further in view of Kruys U.S. Patent No. 5,555,309.

As to claims 11, 22 and 29, Lipner et al does not teach utilizing a plurality of public master keys and a plurality of private master keys to decrypt the encrypted session key.

Kruys teaches a plurality of master keys [column 2, lines 56-67].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Lipner et al so that there would have been a plurality of public and private master keys to decrypt the encrypted session keys. There would

have been multiple session keys so there would have been a public/private master key set to encrypt and decrypt the session keys.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Lipner et al by the teaching of Kruys because it utilizes master keys, each one of which is unique to a respective domain member, and is arranged to protect the respective member vector key of each domain member [column 3, lines 55-62].

Conclusion

9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Aravind K Moorthy whose telephone number is 703-305-1373. The examiner can normally be reached on Monday-Friday, 8:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Aravind K Moorthy
March 16, 2004

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100